# WINET Setup

```
sudo sysctl fs.inotify.max_user_watches=524288
sudo sysctl fs.inotify.max_user_instances=512
```

```
kind create cluster --name wp3 --config /wp3-experiment/Deploy/kind-cluster.yaml --image kind-cni:wp3.v1
```

```
docker exec wp3-control-plane kubectl apply -f
https://raw.githubusercontent.com/projectcalico/calico/v3.25.0/manifests/calico.yaml
```

```
sleep 60
calicoctl delete ippools default-ipv4-ippool
sleep 60
calicoctl apply -f /wp3-experiment/Deploy/ippool.yaml
```

```
calicoctl delete felixconfig default
calicoctl apply -f /wp3-experiment/Deploy/felix_config.yaml
```

```
kind load docker-image bonesi:wp3.v2 snort:wp3.v5 iot:wp3.v2 smd-metrica:wp3.v4 smd-metrica:wp3.v3 --name wp3
```

A rede que contém os agentes malignos mudou do nó 10 para o nó 16

```
docker exec wp3-worker16 sysctl -w "net.ipv4.conf.all.rp_filter=0"
```

Need to modify the ovs network files

```
docker exec wp3-worker2 ip route del default
docker exec wp3-worker2 ip route add default via 192.168.10.2
docker exec wp3-worker5 ip route del default
docker exec wp3-worker5 ip route add default via 192.168.20.2
docker exec wp3-worker8 ip route del default
docker exec wp3-worker8 ip route add default via 192.168.30.2
docker exec wp3-worker11 ip route del default
docker exec wp3-worker11 ip route add default via 192.168.40.2
docker exec wp3-worker14 ip route del default
docker exec wp3-worker14 ip route add default via 192.168.50.2
```

```
# Rede 1
docker exec wp3-worker iptables -A FORWARD -i eth2 -j ACCEPT
docker exec wp3-worker iptables -A FORWARD -i eth1 -j ACCEPT
docker exec wp3-worker ip route add 192.168.20.0/24 via 192.168.0.3
docker exec wp3-worker ip route add 192.168.30.0/24 via 192.168.0.4
docker exec wp3-worker ip route add 192.168.40.0/24 via 192.168.0.5
docker exec wp3-worker ip route add 192.168.50.0/24 via 192.168.0.6
docker exec wp3-worker ip route add 192.168.10.64/26 via 192.168.10.3
```

```
# Rede 2
docker exec wp3-worker4 iptables -A FORWARD -i eth2 -j ACCEPT
docker exec wp3-worker4 iptables -A FORWARD -i eth1 -j ACCEPT
docker exec wp3-worker4 ip route add 192.168.10.0/24 via 192.168.0.2
docker exec wp3-worker4 ip route add 192.168.30.0/24 via 192.168.0.4
docker exec wp3-worker4 ip route add 192.168.40.0/24 via 192.168.0.5
docker exec wp3-worker4 ip route add 192.168.50.0/24 via 192.168.0.6
docker exec wp3-worker4 ip route add 192.168.20.64/26 via 192.168.20.3
```

```
# Rede 3
docker exec wp3-worker7 iptables -A FORWARD -i eth2 -j ACCEPT
docker exec wp3-worker7 iptables -A FORWARD -i eth1 -j ACCEPT
docker exec wp3-worker7 ip route add 192.168.10.0/24 via 192.168.0.2
```

```
docker exec wp3-worker7 ip route add 192.168.20.0/24 via 192.168.0.3
docker exec wp3-worker7 ip route add 192.168.40.0/24 via 192.168.0.5
docker exec wp3-worker7 ip route add 192.168.50.0/24 via 192.168.0.6
docker exec wp3-worker7 ip route add 192.168.30.64/26 via 192.168.30.3
```

```
# Rede 4
docker exec wp3-worker10 iptables -A FORWARD -i eth2 -j ACCEPT
docker exec wp3-worker10 iptables -A FORWARD -i eth1 -j ACCEPT
docker exec wp3-worker10 ip route add 192.168.10.0/24 via 192.168.0.2
docker exec wp3-worker10 ip route add 192.168.20.0/24 via 192.168.0.3
docker exec wp3-worker10 ip route add 192.168.30.0/24 via 192.168.0.4
docker exec wp3-worker10 ip route add 192.168.50.0/24 via 192.168.0.6
docker exec wp3-worker10 ip route add 192.168.40.64/26 via 192.168.40.3
```

```
# Rede 5
docker exec wp3-worker13 iptables -A FORWARD -i eth2 -j ACCEPT
docker exec wp3-worker13 iptables -A FORWARD -i eth1 -j ACCEPT
docker exec wp3-worker13 ip route add 192.168.10.0/24 via 192.168.0.2
docker exec wp3-worker13 ip route add 192.168.20.0/24 via 192.168.0.3
docker exec wp3-worker13 ip route add 192.168.30.0/24 via 192.168.0.4
docker exec wp3-worker13 ip route add 192.168.40.0/24 via 192.168.0.5
docker exec wp3-worker13 ip route add 192.168.50.64/26 via 192.168.50.3
```

**Rede 6 -> DDos**

```
# Rede 6
docker exec wp3-worker16 iptables -A FORWARD -i eth1 -j ACCEPT &&
docker exec wp3-worker16 ip route add 192.168.10.0/24 via 192.168.0.2 &&
docker exec wp3-worker16 ip route add 192.168.20.0/24 via 192.168.0.3 &&
docker exec wp3-worker16 ip route add 192.168.30.0/24 via 192.168.0.4 &&
docker exec wp3-worker16 ip route add 192.168.40.0/24 via 192.168.0.5 &&
docker exec wp3-worker16 ip route add 192.168.50.0/24 via 192.168.0.6
```

```
docker exec wp3-worker16 ip route del 10.128.10.0/24 &&
docker exec wp3-worker16 ip route add 10.128.10.0/24 via 192.168.0.2 &&
docker exec wp3-worker16 ip route del 10.128.20.0/24 &&
docker exec wp3-worker16 ip route add 10.128.20.0/24 via 192.168.0.3 &&
docker exec wp3-worker16 ip route del 10.128.30.0/24 &&
docker exec wp3-worker16 ip route add 10.128.30.0/24 via 192.168.0.4 &&
docker exec wp3-worker16 ip route del 10.128.40.0/24 &&
docker exec wp3-worker16 ip route add 10.128.40.0/24 via 192.168.0.5 &&
docker exec wp3-worker16 ip route del 10.128.50.0/24 &&
docker exec wp3-worker16 ip route add 10.128.50.0/24 via 192.168.0.6
```

```
docker exec wp3-worker16 ip route add 10.128.10.0/24 via 192.168.0.2 &&
docker exec wp3-worker16 ip route add 10.128.20.0/24 via 192.168.0.3 &&
docker exec wp3-worker16 ip route add 10.128.30.0/24 via 192.168.0.4 &&
docker exec wp3-worker16 ip route add 10.128.40.0/24 via 192.168.0.5 &&
docker exec wp3-worker16 ip route add 10.128.50.0/24 via 192.168.0.6
```

```
root@wp3-worker16:/# ip route show
default via 172.18.0.1 dev eth0
10.128.10.0/24 via 192.168.0.2 dev eth1
10.128.20.0/24 via 192.168.0.3 dev eth1
10.128.30.0/24 via 192.168.0.4 dev eth1
10.128.40.0/24 via 192.168.0.5 dev eth1
10.128.50.0/24 via 192.168.0.6 dev eth1
blackhole 10.128.200.0/24 proto bird
172.18.0.0/16 dev eth0 proto kernel scope link src 172.18.0.8
192.168.0.0/24 dev eth1 proto kernel scope link src 192.168.0.20
192.168.10.0/24 via 192.168.0.2 dev eth1
192.168.20.0/24 via 192.168.0.3 dev eth1
192.168.30.0/24 via 192.168.0.4 dev eth1
192.168.40.0/24 via 192.168.0.5 dev eth1
192.168.50.0/24 via 192.168.0.6 dev eth1
root@wp3-worker16:/#
exit
sbrisio@mentored-wp3-vm1:/wp3-experiment/Deploy$
```

Snort drop packet

```
docker exec wp3-worker iptables -I FORWARD -j NFQUEUE --queue-num=20 --queue-bypass
docker exec wp3-worker4 iptables -I FORWARD -j NFQUEUE --queue-num=20 --queue-bypass
docker exec wp3-worker7 iptables -I FORWARD -j NFQUEUE --queue-num=20 --queue-bypass
docker exec wp3-worker10 iptables -I FORWARD -j NFQUEUE --queue-num=20 --queue-bypass
docker exec wp3-worker13 iptables -I FORWARD -j NFQUEUE --queue-num=20 --queue-bypass
```